Contribution to the public consultation on the CNIL's draft recommendation on "cookies and other trackers"

Michael Toth, Nataliia Bielova, Cristiana Santos, Vincent Roca, Célestin Matte

Contribution to the public consultation on the CNIL's draft recommendation on "cookies and other trackers"

Michael Toth, Nataliia Bielova, Cristiana Santos, Vincent Roca,
Célestin Matte (PRIVATICS Inria, France)

February 25, 2020

In this document, we present our opinion on the Commission Nationale Informatique et Libertés (hereinafter, "CNIL") Draft Recommendation "On the practical procedures for collecting the consent provided for in article 82 of the French data protection act, concerning operations of storing or gaining access to information in the terminal equipment of a user (recommendation "cookies and other trackers")" from January 14$^{\text{th}}$, 2020 [5].

We first provide a high-level opinion and feedback on the CNIL draft recommendation, that summarizes our more detailed analysis of various paragraphs of the draft. In the following sections, we first present a quotation from the draft recommendation on cookies and other trackers in a visual box, and then provide our opinion, concerns or open questions. In the **bold text** we emphasize our recommendations. In our reasoning, we often rely on the legal and technical analysis of consent dialogs we have conducted, which is now available as a draft paper [22].

Our opinions

Below, when we cite a paragraph of the draft recommendation (such as "par 6"), we refer to our comment on each paragraph that can be found in the sections below.

Opinion on the environments concerned

- **Mobile environments should be clearly defined, mobile apps should be excluded**. Mobile web browsers have clearly the same concerns as standard desktop web browsers. However mobile applications raise completely different privacy concerns related to data collection than web browsers. The consent is also collected in very different ways in mobile apps from web browsers (par 6) We recommend to remove mobile applications from this recommendation and address them in a different document.

  In the following, whenever we refer to a "mobile application" or "mobile environment", we mean "mobile web browser application".

- **Web browser vendors should also be discussed in this recommendation**. In particular, some browser providers, like Google Chrome, propose logged-in environment to all users by default that facilitates permanent profiling of users. Additionally, and independently of loggin-in, browser vendors can integrate tracking into the browsers, and therefore are obliged to follow the same recommendations on purposes and consent of the CNIL. Such practice is not completely understood

by the research community, nevertheless Google has been observed to integrate unique identifiers into the Chrome browser (par 7).

Opinion on consent in general

- **The scope of consent is not clearly defined** and deserves a more fine-grained recommendation by the CNIL (see par 27).
- **The consent should be standardized**. The standardized consent should be based on four standardized elements: *purposes, categories/types of data collected, data controllers, and trackers that facilitate the data collection*. These building blocks are needed to be defined by Data Protection Authorities for a standardisation of consent:
  - *an exhaustive list of standardized purposes*:
    - the purposes should be human-understood and machine-readable (see par 18, 20). Additionally, a taxonomy of purposes would allow to reason about them (see par 18).
    - which standardized purposes should rely on which legal basis: with standardized purposes, DPAs could set stricter rules on which purposes should be used with consent and which are definitely exempted of consent and under which conditions (par 9 and 10).
  - *categories (e.g., personal, sensitive) and types (more fine-grained description) of data collected should be standardized* (par 23, 25).
  - *standardized presentation of data controllers*, such as the company name, domain URL, privacy policy link, etc.
  - *standardized naming convention for trackers* from a pre-defined vocabulary of names (par 68).
- In a standardized consent, in a given consent scope, **each tracker should have only one standard purpose, categories/types of data collected, list of data controllers and a legal basis applied to it** (par 10 on cookies, par 66 provide suggestions).
- The same standard can be used **to inform the users about the purposes of all the trackers** present on a website independently of the legal basis (see par 17, 68).
- **If consent is standardized, it can be also set in a web browser interface**. Web browser indeed can provide an interface to register a consent pre-defined by the user, using the same standard as other actors (par 73). This will allow the browser to exchange the consent with the data controllers automatically.
- **If the user's choice does not correspond to the expected choices of the data controller, the data controller should provide other means of accessing the same version of the website** (such as paid options), where the user's choice is respected. Blocking or reducing the service provided by the website without other options has detrimental effects (par 36). This also applies to situations when the choice made in the browser interface is more restrictive than the choice expected by the data controller (par 73).

Opinion on design of consent dialogs

- *Neutral* design patterns should be more explicitly defined by data protection authorities as best practices, especially to address the requirement of unambiguous consent (see par 51, 52).
- Moreover, *standard neutral interfaces and design patterns* should be identified by the data protection authorities (see par 39, 42). We suggest a deeper analysis of design patterns that have a direct impact on the user choice (see par 39 and 51).
- The *"consent walls"* [22] force the user to make a choice by blocking access to the website (see par 38). For publishers that provide a free access to the website independently of the user's choice, consent wall is discouraged because it forces the user to make a choice that doesn't influence her

browsing experience. For publishers that provide two or more means of access (such as free and pay), consent wall is allowed if it clearly lets the user to choose between the various options of access.

- In consent settings, *the procedure to refuse should be as simple as to accept.* This applies to the (i) global acceptance and refusal buttons that need to be visually fair and balanced (see par 35), and (ii) the ability to withdraw consent as easily as to give (par 53, 55). The same requirement should apply to the user's choice between accepting and refusing purposes.
- *In the first layer of the consent dialog, the user must be able to* be informed of the scope of consent (par 27), accept or reject high-level purposes (see par 43, 45, 46), and be able to choose between global acceptance or refusal (par 46).
- *Change in user's choice* that includes, but not limited to the withdrawal of consent, should be accessible via a *standard icon* and in *an expected location on the page* (par 56, 57). The change in the user's choice must be communicated to all the concerned parties (par 59).
- *Change in data controllers list* requires that a consent dialog is shown to the user again in case of "qualitatively substantial" changes in the list. Frequent consent dialogs could overwhelm the user. A more concrete definition and examples of "qualitatively substantial" changes should be provided (par 26).
- *Consent validity:* user should be able to choose the validity period of his consent (par 59) and the default duration of refusal should be the same duration as acceptance (par 37).

Opinion on technical characteristics of consent

- The user's choice must be stored in a predefined storage (for example, cookies) with a standard name (see par 69).
- The technical storage of consent should correspond to the choices the user made in the consent interface (par 36, 65).
- Proof of consent: all proofs of consent collection need to be collected: visual proofs (such as videos), code used for consent collection and a proof that the code has actually been deployed in the system in question. Additionally, cryptoprimitives must be used to ensure that the consent has not been forged (see par 61, 64, 65).

In the following sections, we present opinions on different sections and paragraphs of the draft recommendation of the CNIL [5].

On the initial observations

> The purpose of these guidelines was to present the legal framework applicable to storing or the gaining of access to information already stored (hereinafter "trackers") in the terminal of a user or subscriber of an electronic communications service (hereinafter "the user").

This recommendation focuses only on the consent collected for data processing related to "operations of storing or gaining access to information in the terminal of a user". However, it is important to address also other techniques that rely on server-side tracking, such as IP tracking, passive fingerprinting (such as via `User-agent`), whether used alone or in conjunction with the methods discussed here.

1 On the scope of the recommendation (Article 1)

1.1 Environments concerned

6. This recommendation takes particular account of configurations specific to web environments and mobile applications. The examples of compliant practices can however inspire and guide the development of interface in other contexts where the consent provided for in Article 82 of the "French data protection act must be collected (connected television, video game console, voice assistant, etc.).

The Recommendation mentions mobile applications without clarifying if this is restricted to mobile web browsers, or more generally any type of mobile application. If the case of mobile web browsers makes sense, the other mobile applications raise many questions that are probably out-of-scope of this document. For instance, the way personal data is collected by mobile applications (e.g., through libraries proposed by third-parties and included by application developers), the nature of personal data (e.g., various types of UUID/techical identifiers, app name, list of applications, etc.), and the way consent is collected (through static or dynamic application permissions) are quite different from what is discussed in this Recommendation. **It is suggested to clarify what is meant by "mobile environments", and explicitly remove "mobile apps" from this recommendation.**

It is nevertheless interesting to consider the possible adaptation of this recommendation to other environments than web and mobile. It is then necessary to take into account the difficulties resulting from this adaptation. For example, **when the recommendation refers to "voice assistants", we underline that it is necessary to consider that these devices are not equipped with screens or keyboards** and hence the collection of consent is less obvious and requires further analysis and recommendations on its design. In addition, the use of specific hardware devices previously purchased by the user may present an additional risk. Particular attention should be paid to the moment when the engagement of the data subjects begins. In this case, the commitment begins with the purchase of the product. Information concerning the possible collection of personal data, and the possibility to oppose to it, must therefore be provided at the same time (for instance, via easily identifiable icons). Delaying this information at the time of configuration carries the risk of creating a commitment bias in contradiction to the requirement of freedom of consent.

7. The recommendation concerns both environments in which the user is authenticated (sometimes called "logged-in environment") as well as "unlogged" ones. Indeed, the fact that the user is authenticated does not dispense with the need to obtain his or her consent in accordance with Article 82 of the "French Data Protection Act", as long as trackers subject to consent are used.

In "logged-in environments", there is a risk that a website may easily acquire a large amount of information about its visitors, who move around on the pages of this same site without logging out. **Special attention should be paid to systems where extensive profiling of users is easily achievable.** A particular attention should be paid to the following cases:

- The user navigates out of the "logged-in environment", for example by clicking on a link inside the social network and hence visiting an unrelated website. The question is whether the consent provided to the "logged-in" environment extends to the unrelated websites. This refers to the discussion on the scope of consent (see par 69).
- Another problematic use case is "single sign-on" [1]: this allows the login providers to collect information about the visits to various websites, and hence the question of the scope of consent arises in this situation as well.
- It should not be forgotten that the biggest actor in the online advertisement industry (Google) is also a browser provider (Chrome), thus making any "unlogged" session a potential "logged" one for this actor. It's been recently discovered that any Chrome browser session is broadcasting a unique identifier [3].

1.2 Concerned trackers

9. In the light of the practices brought to the Commission's attention, the following trackers may, in particular, be regarded as exempted:

- the trackers keeping the choice expressed by the user on the use of trackers or the will of the user not to express a choice;
- trackers intended for authentication to a service;
- trackers designed to keep track of the content of a shopping cart on a merchant site;
- user interface customization trackers (e.g. for the choice of language or presentation of a service), where such customization is an intrinsic and expected element of the service user;
- trackers allowing load balancing of equipment contributing to a communication service;
- trackers allowing paying sites to limit free access to their content to a predefined quantity and/or over a limited period of time;
- trackers enabling audience measurement, within the framework specified by Article 5 of the Guidelines on cookies and other trackers.

In Table 1 of our draft paper [22], we have analysed the WP29 opinion [17] and identified three more categories that should be exempted of consent: "user security for a service requested by the user", "social media plugin for a functionality explicitly requested by a user" and "session multimedia content player".

Questions to the CNIL: are these categories exempted of consent as well? According to our analysis,

- "user security for a service requested by the user" exemption seems not to apply in case of security of third-party integrated services. A typical example of such cookie would be a cookie set by Cloudflare that "helps detect malicious visitors" for third-party content[1].
- "social media plugin for a functionality explicitly requested by a user" – the current recommendation seems to ensure that this is not exempted of consent.
- "session multimedia content player" seems to be a strictly necessary cookie and hence seems to be exempted.

These points should be clarified in the final document, so as not to leave ambiguous cases.

10. Trackers only fall outside the scope of the consent requirement if they are used exclusively for one of the purposes set out above. A tracker loses the benefit of the exemption if it is also used for another purpose subject to consent.

We completely agree that a tracker loses the benefit of the exemption if it is also used for another purpose subject to consent. This practice is further emphasized in point 66 of the recommendation draft ("How to use cookies: good practices"). A scenario where a tracker that has two purposes, where one requires consent, while the other doesn't, will eventually impact and potentially break the functionality of the website (or mobile application) where it is integrated, if the user decides to refuse the usage of the tracker in the consent dialog.

[1]The cookie policy of Cloudflare describes the purpose of cookie *__cfduid* as "The *__cfduid* cookie helps Cloudflare detect malicious visitors to our Customers' websites and minimizes blocking legitimate users.". Quoted from `https://support.cloudflare.com/hc/en-us/articles/200170156-Understanding-the-Cloudflare-Cookies#12345682` on February 21, 2020.

1.3 Actors concerned

12. This recommendation concerns both the trackers used by the publisher of a website or mobile application and those used by third parties. In the case of a website, the fact that the trackers are deposited via the domain to which the site in question belongs, or via a subdomain of the same publisher, or via the domain of a third party, has no effect on the obligations arising from Article 82 of the "French Data Protection Act" law. The obligation to obtain consent is attached to the purpose of the tracker and not to the technical characteristics of its implementation.

The attachment of the obligation to obtain consent to *the purpose* and not to the characteristics of the user is an essential element of this recommendation – **we fully agree** and also underline this observation in Section 3.3 of our draft paper [22].

13. Both publishers and third parties can be regarded as responsible for the read or write operations. The Commission points out that the controller of the processing operation(s) is the natural or legal person who alone or jointly decides on the purpose and determines the means of the read and/or write operation. This qualification is therefore likely to apply to both:

- to the publisher wishing to meet a need it has defined (e.g. to measure its audience) and appealing for this purpose:
  - to third parties who issues trackers, acting solely on his instructions and on his behalf. In this case, third parties act as subcontractors of the publisher;
  - to trackers that the publisher issues and which it manages on its own;
- to the third party to the site or application consulted by the user, which uses trackers in order to collect data for a purpose it has determined (for example, the third party offers several publishers a service to enrich the data it collects from trackers implemented on different sites or applications).

Such statement seems to imply that the qualification of data controllers can apply independently to either publishers or third parties. This draft recommendation does not explicitly mention joint controllership, despite the recent rulings delivered by the Court of Justice of the EU in the following cases: the Planet 49 judgment [13], the Wirtschaftakademie [11], and the Fashion ID cases [12].
We believe this point should be clarified.

14. The Commission stresses out that the publisher of the site or mobile application whose visit triggers the deposit of trackers, and who therefore authorizes the deposit and use of trackers, including by third parties, from its site or mobile application, should ensure that a mechanism is in place to obtain the free, specific, informed and unambiguous consent of users for the operations of reading and/or writing information in the terminal, in accordance with Article 82 of the Law.
15. In general, the Commission observes that, in many cases, publishers of mobile sites or applications are in the best position to inform users of the information on deposited trackers and to collect their consent, because of the control they exercise over the interface for collecting choices and the direct contact they have with the user.

The draft does not explicitly identify the entity who is –ultimately– responsible for informing and collecting consent from users. The draft departs from the assumption that in general, given that app and website publishers have a direct contact with users and the control they exercise over the consent management interface, they are –in many cases - best suited to inform users and to obtain their consent.

However, publishers have a limited control on the third-party content they include, i.e., they are in control of *what* to include, but not on *what the included content contains*. The responsibility *weighs* only on the publisher side, even if it does not determine the purposes of the cookies, the actors who use them, nor the type of technologies used by these third parties.

We believe **the following questions should be analysed in more depth in concrete systems** (websites, mobile applications or other environments):

1. where is the limit of the publisher's control?

2. when is the responsibility for collecting consent solely on the included content provider?

For websites, we have technically analysed the ecosystem of control and third party inclusion in our recent publication [23].

2 On the requirement for informed consent (Article 2)

2.1 Information on the purpose of trackers

17. The purpose of the trackers must be presented to the user before he or she is given the opportunity to consent or not to consent to their use.

As a good practice, **the purposes of all trackers (also those exempted of consent) should be declared in a visible policy (for example, in a privacy policy)**. This practice needs to be supported because i) the trackers deployed upon a user's visit to a website or installing a mobile app become part of a data processing operation, ii) it is needed for transparency and further auditing.

With respect to cookies, Data Protection Authorities already advocate that *all* cookies could declare their purpose. The ICO (UK DPA) [14] endorses that it is good practice to provide clear information about the purposes of all cookies, including those that are strictly necessary. The 29WP [16] notes that although some cookies may be exempted from consent required by Article 5(3) of the ePrivacy Directive, they may still be used as part of a data processing operation, which means that providers of information society services still have to comply with the obligation to inform users about the usage of cookies prior to their setting.

18. Purposes must be formulated in an intelligible manner, in a sufficiently clear and appropriate language to enable the user to understand precisely what he or she is consenting to. In order to facilitate the reading for the user, the Commission recommends that each purpose be highlighted in a short and prominent title, which would be accompanied by a brief description.

Currently, publishers and third parties are left with a free choice on how exactly to formulate the purposes, and in practice, such free design formulation can lead to misunderstanding and sometimes even manipulation of the end users. As many websites have an identical set of purposes, these could have streamlined formulations. **We therefore suggest that the CNIL (possibly together with other DPAs) proposes a pre-defined standardized taxonomy of purposes**.

Purposes could be modeled using ontologies that allow reasoning about purposes inclusions, implications and generalisations. Such taxonomy of purposes would also help to see when further uses of personal data are compatible or not with the original purposes and will allow a more scalable auditing of websites and mobile app behaviors.

Additionally, we recommend that **a structured machine-readable representation of the purpose of trackers is proposed**. Such machine-readable descriptions (1) allow a direct visual spotting of each purpose, and (2) enables an automatic, large-scale auditing of tracker descriptions for compliance and transparency concerns.

Examples of differing names of purposes are shown below:

- "audience measurement" is also known as "analytics";
- "displaying of advertisement" is also known for "non-personalized advertising", "basic ads", and "ad selection, delivery, reporting";
- "content customization" is also named as "personalization" or "preferences";
- "sharing on social networks" is also known as "social media plugin".

Examples of how to comply with the applicable rules
19.

- If the advertisement is customized according to the precise location of the user (with an accuracy greater than the scale of a city or more than one decimal unit in terms of latitude/longitude), this purpose can be described as follows: "**Geolocation advertisement:** [name of site/app] [and ***third party companies/our partners***] use/use trackers to send you advertisement based on your location"

The threshold of precision beyond which geolocation is considered non-intrusive, "at the scale of one city or more than one decimal precision in latitude/longitude", carries a risk due to differences in population density and mobile coverage. It would indeed be much easier to re-identify a person living in a small town. For this reason, **we believe the reasoning about the accuracy has to be done in terms of anonymity sets (number of people in a given location unit) rather than in terms of decimal precision**.

20. In order to enable the user to understand more precisely what he or she is consenting to, the Commission recommends that, in addition to the list of purposes presented on the first screen, a more detailed description of these purposes is included in an easily accessible way in the consent collection interface. In practice, this information can be displayed under a scroll button that the user can activate directly at the first level of information. It can also be made available by clicking on a hyperlink at the first level of information

Only in this statement implies that the purposes for data collection must be presented on the first screen. **We recommend that the high-level purposes are indeed shown to the user at the first screen of the consent dialog.**

The draft proposes that a detailed description of purposes is easily accessible from the first screen via "a scroll button that the user can activate directly at the first level of information". We suggest to include the detailed description of each purpose in the privacy policy that is easily accessible by manual and automatic means. The UK DPA (ICO) makes such suggestion *'You also need to specify your purposes in your privacy information for individuals'* [15]. **We invite the CNIL and DPAs to propose a standard relative path on the server host, such as "/privacy-policy" and a structure of a privacy policy that can be analysed by machines**. Similar self-declarative approaches have been already used in the past for websites: the declaration of access to crawlers in `robots.txt` file [21] and declaration of advertisers recently in `ads.txt` file [2].

Figure 2 - Details of the purposes are available by clicking on a hyperlink on the first level of information
21. Regarding the content of this additional information and, as an example, with regard to the display of advertisement (personalized or not), it can be specified that this purpose encompasses various technical operations such as the display of advertising, the capping of the display (sometimes called "advertising capping"), aiming at not presenting the same advertisement to a user in a repetitive manner, fighting against click fraud (detection of publishers claiming to have a larger advertising audience than they actually do), billing the display services, measurement of the size of the targeted audience, better understanding the audience, etc.

Even though the proposed example enables the identification of an "overall purpose" and the "related purposes" or related processing operations (under whose umbrella a number of related processing operations take place), **we do not fully agree with the example in Figure 2 due to usability and user's expectations and reactions to such consent dialog**.

The technical explanation of targeted advertisement on the right-hand side of Figure 2 presents several activities, such as "displaying the ad" or "frequency capping". Such technical descriptions are not necessarily useful for the users to make their choice regarding their consent. However, such descriptions can scare the users, thus increasing the chance that they will consent to targeted ads. The primary goal of

end users is to visit their websites (or use their apps), therefore if the consent mechanism might influence their satisfaction with the website, users will be more likely to accept the consent. As such, the purpose of not presenting the same ad to a user in a repetitive manner may let users think that their website experience will worsen if they refuse consent (because they will start seeing the same ads many times) and therefore will guide them to accept an overall "targeted advertisement" purpose that include a vast user's data collection.

23. Finally, as a good practice, the categories of data collected through trackers could be specified for each purpose in a way that is easily accessible to the user.

We believe the categories of data collected must be specified for each purpose. This becomes particularly important when the special categories of personal data are collected or used.

It is however important to identify whether the categories of data collected should be visible at the first or the second layer of information. **For consent to be informed, users should be able to see what data is collected about them at the first layer of information.**

Additional recommendation on consequences of purposes.

Additionally, as a general comment to the section 2.1 of the draft, and as a best practice, **we recommend that the *consequences* of the purposes are defined and shown to the user**. This is especially important for the purpose of "behavioral advertising" which entails profiling. The CNIL acknowledges that *Online advertising profiling can be massive and perceived as intrusive* [6] and for this reason, showing the resulting consequences of such processing could enable the data subject's control and awareness over his personal data.

2.2 Information on data controllers and the scope of consent

24. The user must be able to find out the identity of all those responsible for the processing operation(s) before being able to give consent or refuse to give his or her consent. He or she must therefore be fully aware of the effective scope of his or her consent.

The draft does not explain what is "the scope" of consent. **We recommend that an intuitive example of a scope is proposed**.

25. Pursuant to this requirement, the exhaustive list of controllers of the processing operation(s) should be made available to the user upon obtaining consent and permanently made easily accessible.

We welcome this practice for an informed consent (which is already ruled in the Planet 49 judgment [13]) and for which is required a clear definition of the *role* of the actors (data controller, joint data controllers), as we mentioned in the section 1.3 (Actors concerned).

Additionally, **the categories and types of data collected by each controller and the purposes should be clearly visible for the user**. In the state of the art of cookie banners, we often observe lists of third parties, however it does not help the user to make an informed choice because the user does not know what type of information these parties collect and for which purpose.

26. In addition, this list should be regularly updated. In order to avoid overburdening the user, the Commission considers that in case of additions that are qualitatively nonsubstantial, it is sufficient that the updated list of controllers of the processing operation(s) is made available to the user via a permanent and easily accessible link on the service, e.g. through the consent removal mechanism. On the other hand, in the case of a substantial addition, the user's consent should be sought again before continuing with the reading and/or writing of information on his terminal equipment.

The concept of "qualitatively non-substantial" seems vague, open to different interpretations and implementations per website, which can trigger confusion for the user. **It would be useful to provide a standard definition and a list of examples of "substantial" and "non-substantial" changes**.

27. Finally, for the user to be fully aware of the scope of his or her consent, he or she should particularly know whether the consent is valid for the tracking of his or her navigation on sites or applications other than those on which his or her consent is collected. Information on the extent of navigational tracking permitted by the trackers, indicating the different web sites and applications concerned, should be made available to the user before he or she expresses a choice.

The scope of the consent is essential and deserves more attention: we agree that the first question to be asked is if whether the scope is restricted to the website, or if tracking continues when visiting other websites after having consented. Additionally, we further ask: is the scope restricted to the tab from which the user consented? For instance, if a user closes the tab from which he consented, what will be the consequences: is the controller still able to track him on other tabs or not? And if the user closes the web browser session altogether, and then starts a new session, is the controller able to track him again? Regarding browsing history, does the consent apply to whatever is stored in the browser (included sites accessed in the past if available), or only to the new browsing history? The notion of scope of the consent is pretty complex and obscure to a user.

28.In practice, in order to reconcile the requirements of clarity and conciseness of information with the need to identify all those responsible for the processing operation(s), specific information on these entities (identity, link to their privacy policy) may be given on a second level of information. They can be made available on the first level via, for example, a hyperlink or a button accessible from this level. The Commission recommends using a descriptive name and using clear terms such as "list of companies using trackers on our website/application"

It's not practical to assume that users will explore the privacy policy of each controller, especially because the number of controllers on each website can reach several hundreds (this is the case for consent dialogs that implement IAB Europe Transparency and Consent Framework [8, 7]. **We recommend that the information about each controller, the data it collects and the purposes thereto are presented in a precise and easily understandable form**.

30. Finally, for a consent (which is collected on one site or mobile application) to also be valid on other sites or mobile applications, the list of all the websites or mobile applications concerned can be made accessible via a hypertext link or a button located on the first level of the consent collection mechanism.

When consent is shared between several sites or mobile applications, it is necessary to ensure that this does not generate further transfer data to the site, such as the list of sites previously visited by the user. **We recommend adding precise rules for the shared consent, to avoid leakage of information via this mechanism.**

32. With regard to the modification of the list, the fact that the list has been modified could be usefully highlighted, for example by a change of colour of the link leading to it, or a particular animation of that link. Within the list, it is possible to draw the user's attention to the controllers of the processing operation(s) that have joined the list since the last expression of consent, so that the user can maintain consent in full knowledge of the facts.

We agree that highlighting a change in the list by changing the color of the link pointing to it can bring user's attention. However, new information of the list might overwhelm the user, because he'll need to recall to whom consent was given before, but also reason about new controllers and what has possibly been changed. If there are changes, they should be shown to the user in the least intrusive way: for example, by showing only new controllers. However, in order to compare "old" and "new" controllers of the list, consent must have a well-defined form.

Additional recommendation on informed consent (Article 2). For readability issues, it would be relevant to provide a graphic representation of links between data controllers – personal data collected – purposes –consequences of such purposes – legal basis, such as those proposed by tools like Polisis and CookieViz.

3 On the requirement for free consent (Article 3)

> 34. In the first place, the person responsible for the processing operation(s) should offer the user both the possibility of accepting and not accepting (in other words, of refusing) the read and/or write operations.

> 35. Secondly, the same degree of simplicity should apply to the ability to consent or not to consent. The ability to express refusal as easily is indeed the counterpart of the ability to express free consent. Therefore, in order not to affect the user's freedom of choice, the mechanism for expressing consent should be presented at the same level and in the same technical manner as the mechanism for expressing refusal.

On the equivalent possibilities if accepting and refusing. **We agree that a sufficient level of granularity of choice is demanded in the website design. We also agree that the choice between "accept" and "reject" must be fair and balanced**. We have highlighted this need in the section 4.5.2 of our draft paper [22]. The Spanish DPA also supports this approach of a balanced choice in their recent decision [4].

> 36. Thirdly, the user should not suffer any prejudice if he or she chooses to refuse. [...] Failure to record the refusal to consent could therefore have the consequence of exerting pressure that could influence his or her choice, thus calling into question the freedom of the consent he or she expresses.

We agree that the user should not suffer any prejudice if he or she chooses to refuse. **Some detrimental practices could be forbidden and explicitly mentioned in the recommendation**, such as the ones we provide below (our examples here are for websites but could applied to other environments as well):

- When users, even before expressing any choice, face a *cookie wall* blocking access to an online service's content (e.g. stating "to access our site you must agree to our use cookies");
- When there is no immediate blocking to the website, however after refusing, user has denied access to the website he wants to visit and no other options for visiting the website are provided;
- "Redirection": when the user refuses tracking, he is redirected to another website or another page of the same website – the user is "tricked" to believe that the website originally requested by the user is unavailable even though it is accessible (however only technology-savvy users would be able to discover this);
- When the consent form or the privacy policy requires the user to install software to express his refusal.

> 36. [...] Indeed, failure to register the refusal would prevent it from being taken into account in the long term, in particular during new visits. If the choice that the user has expressed is not registered, he or she would be asked again to consent. This continued pressure would be likely to cause the user to accept out of weariness. [...]

We agree and underline that the consent that the user chooses in the user interface should be identical to the consent that gets registered by the website, as we propose in the section 4.5.4 of our draft paper [22]. If consent is correctly registered, the user will not be pressured to choose again by the same website even when the user has made a choice visiting it in the past.

Using the open source Cookie Glasses tool[2] [9], it is possible to verify whether consent records the user's choice given in the user interface for consent banners that implement IAB Europe Transparency and Consent Framework v1.0 [7].

[2]Browser extension tool available at <`https://github.com/Perdu/Cookie-Glasses`>

37. Moreover, in the light of the above, the Commission considers that for consent to be freely given, its counterpart, namely the refusal, should be registered (and therefore taken into account) for a duration which is at least identical to that for which consent is registered. In order to preserve the choices expressed by the Internet user, a tracker may be used, with the sole purpose of storing consent or refusal.

We completely agree and support this position of the CNIL.

38. Moreover, nothing prohibits the person responsible for the processing operation(s) to provide the user with the possibility of not making any choice and delaying his or her decision, as long as the user is given the choice between acceptance and refusal. The situation in which the user does not express any positive choice must be distinguished from the situation of refusal. In the absence of any manifestation of choice (neither acceptance nor refusal), no trackers requiring consent should be written. The user could then be asked again as long as he or she does not express a choice.

The last sentence of the draft implies that the user will be forced to respond and express her choice eventually. The draft does not describe whether "consent walls" are discouraged – a consent wall is a mechanism that blocks access to the website/app until the user expresses her choice regarding consent. **We emphasize the need to state clearly whether consent walls are allowed or not. We state they are unnecessary disruptive to the use of the service** (see Section 4.6.2 of our draft paper [22]).

39. Finally, these interfaces should not use potentially misleading design practices, such as the use of visual grammar that might lead the user to think that consent is required to continue browsing or that visually emphasizes the possibility of accepting rather than refusing.

We suggest that the CNIL and researchers define *neutral* design patterns and a (non-exhaustive) list of possible misleading design practices that could impact a freely given consent. In the statement above, the draft only mentions two misleading designs practices: misconception that refusing consent leads to the breakage of the website and manipulation of the user towards accepting because of a structural or coloring scheme (such as bigger or brighter "accept" button and smaller or shadowed "refuse" button).

42. The development of standardised interfaces operating in the same way and using a standardised vocabulary would make it easier for users to understand when navigating from one site to another.

We agree with this best practice of standardized interfaces operating in the same way. Such standardization of design choices would enable an automatic verification of this configuration requirement.

4 On the requirement for specific consent (Article 4)

43. The user must be given the opportunity to give independent and specific consent for each separate purpose.

We agree with this requirement of a separate consent per purpose, already consolidated in the GDPR (in Article 4(11) and in Recitals 32 and 43), the 29WP [19, 18, 20] and in the Planet 49 ruling [13]. We have also proposed this requirements in section 4.3.1 of our draft paper [22].

While the option to consent per purpose complies with the requirement for specific consent, studies on this topic show that it is rarely used [24]. Similarly, the elements presented on a second level of information are generally ignored by users [10]. It is therefore important to **place high-level purposes on the first level of information**, in order to remain accessible to the users, without overloading them with dense and complex information.

45. The Commission considers that the obligation to obtain specific consent does not preclude the possibility of offering the user the ability to consent globally for a range of purposes, provided that:

- all the purposes have been presented to the user beforehand;
- the user is also allowed to consent purpose per purpose;
- the user is provided with the option to refuse globally at the same level and under the same conditions as the option to consent globally.

46. Thus, in order to facilitate the navigation of the Internet user, it is possible to propose global acceptance and refusal buttons via, for example, the presentation of buttons entitled “accept all” and “refuse all”, “I authorise” and “I do not authorise”, “I accept all” and “I do not accept anything” or “I agree to all purposes” and “I do not agree”, allowing him to consent or refuse, in a single action, to several purposes. However, in order to ensure that the user has not been induced by design choices to accept rather than to refuse, it is recommended to use buttons and a font of the same size, offering the same ease of reading, and highlighted in the same way.

Figure 5 - It is possible to offer global accept and reject buttons, for example by presenting "accept all" and "reject all" buttons that are equally emphasized.

We welcome this practice of a global consent to accept and a global consent to refuse, with the specifications given above. Nevertheless, we underline the importance of presenting only high-level purposes beforehand, that are easily understood by the users, do not overload the user with information and do not “trick” the user into believing that refusal may lead to negative consequences.

49. The possibility for users to be able to choose specifically not only by purpose but also by data controller could contribute to strengthening the user’s control over his/her data.

We agree that the user should be able to choose per purpose. Regarding the possibility to choose by *data controllers*, a best practice consists of choosing per category of third party, as suggested by the 29WP (WP259 rev.01) [20]. However, choosing by data controller (be it either the website publisher or third parties) and showing the full list of potential controllers could configure a deceptive design related to information overload. We further describe with more detail in section 4.3.2 of our draft paper [22] the reasons why this practice should not become mandatory.

5 On the requirement for unambiguous consent (Article 5)

51. By its presentation, the mechanism for obtaining consent must enable the data subject to be aware of the goal and scope of the act enabling him or her to signify his or her agreement or disagreement. Thus, this mechanism should not involve potentially misleading design practices, such as the use of visual grammar that impedes the user’s understanding of the nature of his or her choice.

Both this paragraph, and paragraph 39 of the draft mention “potentially misleading design practices”. **We suggest that *neutral* design patterns should be more explicitly defined by the DPAs as best practices**. With respect to user consent, we suggest even a deeper analysis of design patterns that have a direct impact on the user choice.

52. A consent request made using check boxes, unchecked by default, is easily understood by the user. The person responsible for the processing(s) may also use sliders, deactivated by default, if the choice expressed by the user is easily identifiable. The information accompanying each actionable element for expressing consent or refusal should be easily understandable and should not require any effort on the part of the user. Thus, it should not be written in such a way that a quick or careless reading might suggest that the selected option produces the opposite of what the user intended to choose.

To avoid behaviors presenting a margin of doubt regarding the choice expressed by the user, **we suggest that a (non-exhaustive) list of ambiguous behaviors is explicitly mentioned**, as we initially proposed in the section 4.5.1 of our draft paper [22], such as:

- Presumed or implied consent from inactivity or silence on the part of the data subject, e.g. "This website uses cookies to improve your experience. Find out more";
- Proceeding with a service, e.g. "We've placed cookies on your device to help make this website better. By continuing to use the site we assume you consent to this", or "We use cookies to give you the best online experience. By accessing the website, you give your consent to our use of cookies";
- Disappearance of the cookie banner without an affirmative action of the user, and a positive consent is registered by the fact that the user scrolled the website, visited other pages, clicked on links or other actions on a website;
- When the action of closing a banner leads to the registration of a positive consent;
- The only options are accepting consent or closing the banner (even if closing means registration of refusal);
- Only accepting and a link with a "more information" is presented to the user (even though "more information" actually eventually allows the user to make her choice);
- Use of pre-ticked boxes for positive consent.

6 On withdrawal and duration of consent (Article 6)

53. Users who have given their consent to the use of trackers must be able to withdraw it at any time. The Commission reminds that it must be as simple to withdraw as it is to give consent.

We agree that withdrawal must be done at any time and with the same easiness as to give it.

55. In practice, the Commission recommends that solutions allowing the user to withdraw consent should be easily accessible throughout the use of the service. The simplicity of access can be measured by the time spent and the number of actions required to access the withdrawing mechanism.

As a best practice, **the draft should define a list of *criteria*, as well as an ideal threshold**, to assess the envisioned "simplicity" and "easiness" that the draft recommendation proposes. The draft only mentions: i) time spent, ii) number of actions required. **We also suggest the following**:

- possibility to withdraw consent by the *same means* it was asked;
- underline that it is needless to ask the user to state the reason for withdrawing consent;
- we recommend that a maximum timing and the number of actions needed. The use of a procedure requiring more time or actions than this maximum should be justified.

56. The possibility of withdrawing consent may, for example, be offered via a link accessible at any time from the service concerned, in order to ensure that users can withdraw their consent with the same ease as they gave it. It is recommended to use a descriptive and intuitive name such as "cookie management module" or "manage my cookies" or "cookies", etc. The publisher of a website can also provide the user with a configuration module accessible on all the pages of the site by means of a "cookie" icon, located at the bottom left of the screen, enabling him to easily withdraw his consent.

1. **We suggest that the "withdrawal tool" should be named appropriately and should be standardized for all environments (including web and mobile)**. The "cookies" name or "cookie" icon can be misleading, as it does not render an intuitive nor descriptive function of the possibility of revoking the choice made.
2. **We welcome the idea of an icon**. However, the icon design should be standartized and agreed upon to avoide confusion and further potentially misleading design. We have observed one "withdrawal icon" on the `faktor.io` website (see Figure 27 in section 4.7.1 of our draft paper [22]) in a shape of a fingerprint.

57. In any event, the Commission recommends that the mechanism for withdrawing consent be placed in an area that attracts the attention of users or in areas where the user expects to find it, and that the visuals used be as explicit as possible.

We agree with this statement. The option to withdraw consent could be easily accessible, and it may be best to show it in the same place as the consent dialog, as this is probably where users expect to find it.

59. In general, the Commission considers that a period of validity of six months from the expression of the user's choice is appropriate.

- We believe that it is useful to predefine a default validity period of 6 months. Nevertheless, the phrasing does not clearly state whether the validity period applies to the user's choice or only to the positive consent. We recommend to make this statement more explicit so that there is no room for interpretation of the validity period in case of refusal. Moreover, **we would recommend that the user is given the ability to configure the limit of validity of their consent and, in the case of refusal, to be able to make it permanent.**
- The draft recommendation does not specify the retention period applicable to personal data collected through trackers. This absence would therefore implicitly give data controllers the possibility to determine the retention period of personal data themselves. **We suggest to add a discussion on where and how the retention period of the personal data collected is defined and how the user could make his choice regarding the retention period.**
- Withdrawal of consent applies not only to the publisher but also to all the third parties that have collected user's data. **Hence withdrawal of consent has to be communicated to all the concerned parties that have previously received consent**, and the time of communication of withdrawal should be identical to the time of communication of a positive consent. We have underlined this requirement in section 4.7.2 of our draft paper [22].

7 On the proof of consent (Article 7)

61. The controller of the processing operation(s) must therefore be able to:

- on the one hand, provide individual evidence of the collection of user consent; and on the other hand, demonstrate that the mechanism that collected the consent has all the characteristics that allows a valid consent to be collected (freely given, specific,informed and unambiguous), thus providing proof of the overall validity of the consent collection process.

We draw attention of the CNIL to the fact that in some of the existing consent collection mechanisms, such as IAB Europe Transparency and Consent Framework [7], there is no mechanism to protect the integrity of the user's consent when it is shared among several parties. **We recommend the usage of cryptographic primitives to ensure that the choice of the user has never been forged.**

64. The Commission reminds that if the obligation to prove consent leads to the collection of data on the context in which consent was given, it should not lead the controller of the processing operation(s) to collect more data on the user; only data necessary to prove consent should be collected.

We support this proposal and underline that the collection of consent should not lead to revealing the user's browsing history to the party that collects consent; for example, a setting where a cookie registers consent and is set by a third party domain, would allow the latter to learn the browsing history of the user.

65. With respect to proving the validity of the consent, the Commission recommends the following procedures:

- Proof of the validity of the consent may be obtained by placing the code used by the organization collecting the consent, for the different versions of its site or mobile application in an escrow managed by a third party; or
- A screenshot of the visual rendering displayed on a mobile or desktop device can be kept for each version of the site or application; or
- Regular audits of the consent collection mechanisms implemented by the sites or applications from which consent is collected may be implemented.

We believe that a screenshot is not a sound procedure to prove the conformity of the tool because consent collection is often done in several steps and therefore requires video recording. Moreover, the visual proof only demonstrates the interface of the consent collection, but does not show the technical details of its implementation in a concrete system, and therefore could only partially demonstrate the validity of consent. The code used by the organisation moreover, should be able to demonstrate that the code submitted to the escrow is indeed the one used in practice.

The proof of validity should contain a combination of the technical implementation (the code used to collect consent) and the visual representation (videos of obtaining consent) in order to verify both visual and technical requirements on a valid consent. Moreover, the choice of the user in the consent interface must correspond to the technical user's choice sotred in the system. We discuss this in our comments to paragraph 36.

8 On how to use the technologies (Article 8)

66. In order to ensure the greatest transparency in the use of cookies, the use of different cookies for each distinct purpose would allow the user to distinguish between them and to ensure that his consent is respected, but also to make reading or writing operations more transparent. In particular, trackers previously listed as exempt from consent should preferably be used for a single purpose only, so that the lack of user consent does not affect the use of trackers necessary for navigation.

We welcome this good practice: each tracker (including cookies) need to be used for a single purpose – this will allow users to better understand the usage of trackers and bring more transparency to their use. Such recommendation has been already proposed in paragraph 10 of the draft for all trackers that require consent.

Additionally, and more specifically to browser cookies: cookies that require consent should not be merged with third-party content that provides main functionalities to a website. If such cookies are

merged, the browser will automatically send such cookie with every request to fetch third-party content needed for the website to function. As a result, the website has to i) either rely on a consent collected by the third-party when such cookie was stored (and hence illegal consent collection impacts the legality of the website), or ii) request consent before fetching the functional third-party content, thus making the website functioning conditional to the consent of the user. We believe that a more general conclusion is preferable: **trackers that require consent should not be associated with content that is exempted of consent.** We provide a deeper analysis of this scenario in Section 5 of our draft paper [22].

67. The Commission also encourages against the use of entity identity masking techniques using trackers, such as CNAME cloaking.

We welcome this practice regarding the use of masking techniques. We agree that design making data processing more difficult to understand for data subjects should be avoided.

68. The Commission also recommends, as a good practice, that the names of the trackers used should be explicit and, as far as possible, standardised regardless of the actor setting them.

We welcome this good practice of making the name of the trackers explicit and standardizing their denomination. In case of web browser HTTP cookies, **we suggest**:

- a *naming convention* (a generally agreed scheme) vocabulary to name trackers, in order to facilitate their identification as trackers. The use of a naming convention would also help website publishers to label their cookies in an intelligible and standardised way;
- mentioning of the name of the cookie in an easily accessible cookie policy, for transparency and auditing purposes;
- a structured presentation of the name and purpose of each cookie that is easily readable by humans and machines. In this way, it is easy for the data subject to identify the purpose corresponding to each cookie. Such structure also enables large-scale automated studies for cookie and purpose auditing. The ICO [14] holds the same positioning: large tables and detailed lists of all cookies operating on a website may be the type of information that users will want to consider.

69. The Commission also recommends, as a matter of good practice, that the tracker used to store the choice of the user is named "eu-consent", setting each purpose to a "true" or "false" boolean value reflecting the user choice. In the event that the user does not wish to express himself, the tracker can store the number of pages viewed by the user or a reference date in order to limit the resurfacing frequency of the consent collection interface.

We support this practice of naming convention for trackers that store the user's choice. However, in order to encode the user's choice regarding each purpose, the purposes have to be standardised and readable by machines.

Additionally, the browser vendors should not eliminate the storage of the user's choice (such as the "eu-consent" storage) when the user closes the browser. Otherwise the user's choice is eliminated and the user is presented with consent dialogs every time he re-starts the browser. The naming convention will allow browser vendors to avoid this situation by adding exception to the dedicated storage.

Moreover the user should have an easy access to her stored "eu-consent" storage in the web browser in order to check the choice the user already provided in the past for the scope it was given for. We further discuss the possibility to change the user's choice directly in a browser in our comments to paragraph 73 (Article 9).

70. Finally, standardised icons could be developed to enable users to be informed quickly and efficiently.

The use of standardized icons and visuals are a good practice, provided that these icons are offered (or certified) by organizations such as data protection authorities, standards committees, and not by the advertising industry alone. **We suggest that the CNIL proposes such icons**.

9 On the collection of consent via browsers (Article 9)

> 73. Thus, as a good practice, where browser providers and operating systems decide to offer such mechanisms to the user, the Commission recommends that they:
>
> - allow users to consent to, or refuse, read or write operations when first using the browser or terminal concerned, providing they received the information that allow them to make an informed choice;
> - include a mechanism that allows mobile site and application publishers to request and obtain consent in accordance with regulations;
> - where the user has explicitly consented through the above-mentioned mechanism, apply this consent by authorizing the recipient of this consent to perform the read and write operations.

We welcome the proposal of a browser-based consent collection. It allows data subjects not to be over-solicited, under several conditions. First, the browser vendors must use the standardized consent, proposed by the data protection authorities and globally deployed. Browser vendors should follow the same requirements on the design and technical storage of consent as other actors (see par 69).

When the choice made in the browser interface is more restrictive (allows less) than the choice expected by the publisher, two options are possible. First, the publisher can accept this choice without reducing the service and thus having detrimental effects (par 36). Second, the publisher can provide alternative means of access (such as paid options) where the user's choice is respected.

References

[1] Single sign-on, wikipedia page.

[2] Ads.txt specification. `https://iabtechlab.com/ads-txt/`.

[3] Thomas Claburn. Is chrome really secretly stalking you across google sites using per-install id numbers? we reveal the truth, Feb 2020. `https://www.theregister.co.uk/2020/02/05/google_chrome_id_numbers`, accessed on 2020.02.21.

[4] Agencia Española de Protección de Datos. Procedimiento: Ps/00300/2019 – resolucion r/00499/2019 de terminacion del procedimiento por pago voluntario, 2019. `https://www.aepd.es/es/documento/ps-00300-2019.pdf`, accessed 11 December 2019.

[5] Commission Nationale Informatique et Libertés (CNIL). On the practical procedures for collecting the consent provided for in article 82 of the french data protection act, concerning operations of storing or gaining access to information in the terminal equipment of a user (recommendation "cookies and other trackers"). `https://www.cnil.fr/sites/default/files/atoms/files/draft_recommendation_cookies_and_other_trackers_en.pdf`.

[6] Commission Nationale Informatique et Libertés (CNIL). Cnil launches a public consultation on its draft recommendation on "cookies and other trackers", Jan 2020. `https://www.cnil.fr/en/cnil-launches-public-consultation-its-draft-recommendation-cookies-and-other-trackers`.

[7] IAB Europe and IAB Tech Lab. Transparency and consent framework. `https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework`, accessed on 2019.05.03, 04 2018.

[8] IAB Europe and IAB Tech Lab. Transparency and consent framework (v2). `https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/tree/master/TCFv2`, accessed on 2020.01.28, 08 2019.

[9] Célestin Matte, Cristiana Santos, and Nataliia Bielova. Do cookie banners respect my choice? measuring legal compliance of banners from iab europe's transparency and consent framework. In *IEEE Symposium on Security and Privacy (IEEE SP 2020). Accepted for publication.*, 2020.

[10] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In *CHI*, 2020.

[11] European Court of Justice. Case c-210/16 wirtschaftsakademie schleswig-holstein, ecli:eu:c:2018:388, Jun 2018. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-210/16.

[12] European Court of Justice. Case c-40/17 fashion id gmbh & co.kg v verbraucherzentrale nrw ev, ecli:eu:c:2019:629, Jul 2019. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-40/17.

[13] European Court of Justice. Case c-673/17 verbraucherzentrale bundesverband v. planet49, ecli:eu:c:2019:801, Oct 2019. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-673/17.

[14] Information Commissioner's Office. Guidance on the use of cookies and similar technologies, 2019. https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/.

[15] Information Commissioner's Office. Principle (b): Purpose limitation, 2019. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/.

[16] Article 29 Data Protection Working Party. Opinion 16/2011 on easa/iab best practice recommendation on online behavioural advertising, 2011. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.

[17] Article 29 Data Protection Working Party. Opinion 04/2012 on cookie consent exemption, 2012. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[18] Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation, 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[19] Article 29 Data Protection Working Party. Working document 02/2013 providing guidance on obtaining consent for cookies, Oct 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.

[20] Article 29 Data Protection Working Party. Guidelines on consent under regulation 2016/679 (wp259rev.01), Apr 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[21] https://developers.google.com/search/reference/robots_txt.

[22] Cristiana Santos, Nataliia Bielova, and Célestin Matte. Are cookie banners indeed compliant with the law? deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners, 2019. Available at https://arxiv.org/abs/1912.07144.

[23] Dolière Francis Somé, Nataliia Bielova, and Tamara Rezk. Control what you include! server-side protection against third party web tracking. In *International Symposium on Engineering Secure Software and Systems*, pages 115–132, 2017.

[24] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un)informed consent: Studying GDPR consent notices in the field. In *Conference on Computer and Communications Security*, 2019.